Negocio Electrónico

Tema 5. Retos y estrategias de Ciberseguridad en la empresa

Profesorado

Antonio Muñoz Gallego

amunoz@lcc.uma.es

Resumen

- Este tema proporciona una visión general de los aspectos de ciberseguridad en entornos empresariales.
- Se justificará la necesidad de una actuación global y rigurosa, y se mostrará como los beneficios superan los costes.
- Se presentarán las amenazas, las defensas y las posibles estrategias a adoptar.

Introducción

Preliminares

- Tradicionalmente
  - Security
  - Safety
  - Reliability
  - Privacy
  - Accountability
  - Quality
  - ...
- Hoy
  - Non-functional aspects (o Quality, o como queráis)
    - IT Security
    - Safety
    - Reliability
    - Privacy
    - Acountability
    - Quality
    - ...

Preliminares

5ª generación ?
- Computadores globales
- Ubiquitous/Pervasive/AmI
- SOC y Cloud Computing
- CPS, IoT, …

4ª generac
- Sistema
- PCs + internet
- Tecnología OO
- Paralelismo

3ª gen
- AI
- Hw de bajo coste
- Sistemas distribuidos

2ª generación
- Multiusuario
- Tiempo real
- Bases de datos

1ª generac
- **Por lot**
- **Monousuario**
- **Software a medida**

Preliminares

- **Sistemas abiertos**
  - distribuidos, heterogéneos, *evolutivos y de gran escala*
- **Desaparición del control y posesión centralizados**
- **Fin de los conceptos de sistema y aplicación**
- **Incremento de las necesidades de seguridad, privacidad y resistencia**
- **Incremento de la adaptabilidad y sensibilidad al contexto**
- **Self-***

5ª generación ?

- Computadores globales
- Ubiquitous/Pervasive/AmI
- SOC y Cloud Computing
- CPS, IoT, …

Introducción

- **Estamos en una situación desalentadora: aún no tenemos procesos de ingeniería integrales, rigurosos, basados en la experiencia y asistidos por ordenador para ayudar a los desarrolladores de sistemas ciberfísicos en la formidable tarea de diseñar y mantener razonablemente seguros esos sistemas.**

Introducción

- **Los sistemas de control industrial (ICS) y los sistemas de adquisición de datos y supervisión de control (SCADA) han sido objeto de ataques desde hace tiempo.**
- **La introducción de las redes inteligentes (Smart Grids) lleva consigo un elevado riesgo de ataques**

HAVEX

The HAVEX malware is not new, but it has been modified several times since its first reported deployment. It has targeted the energy sector since "at least August 2012."[44] Originally, HAVEX was distributed via spam email or spear-phishing attacks.[45] This new version of HAVEX appears to have been designed as a Trojan horse specifically to infiltrate and modify "legitimate" software from ICS and SCADA suppliers, adding an instruction to run code (i.e., the "*mbcheck.dll*" file) containing the HAVEX malware.[46]

BlackEnergy

In October 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) announced that several industrial control systems had been infected by a variant of a Trojan horse[36] malware program called BlackEnergy.[37] Originally designed for "nuisance spam[38] attacks," the software for BlackEnergy was first reported in 2007 and is designed to target critical energy infrastructure.[39]

Fuente: Cybersecurity Issues for the Bulk Power System
Richard J. Campbell
June 10, 2015

Introducción

- **Nuevos sistemas complejos ▸**
  - Nuevos problemas de seguridad, problemas más complejos, …
- **Las soluciones de seguridad no deben únicamente prevenir los ataques informáticos, sino también los humanos, de ingeniería social (e.g. phishing, etc.) y los físicos.**
- **Seguridad Software vs. Seguridad de la Información vs. Seguridad de Sistemas.**
- **Programación segura vs. Diseño seguro vs. Ingeniería de seguridad.**

Introducción

- **La cosa irá a peor:**
  - Los sistemas de información futuros tienden a ser **compuestos**, **dinámicos**, muy **complejos** y altamente **interconectados**;
    - *van a estar presentes en todos los aspectos de nuestras vidas;*
    - *y serán el objetivo de atacantes poderosos y altamente motivados.*
  - Los sistemas ciberfísicos establecen un puente entre el mundo cibernético y el mundo real.
  - Este puente puede usarse para atacar el mundo real desde el ciberespacio, con la impunidad, conveniencia y comodidad que ello supone.

Ciberasesinos?

Introducción

- **Clasificando las formas de tratar la seguridad**
  - Según el **momento:**
    - ***A priori*** *(aka "by-design")*
    - ***A posteriori*** *(aka "penetrate and patch")*
  - Según la **cobertura:**
    - ***Total*** *(aka "Paranoid")*
    - ***Selectiva*** *(aka "Best effort")*
  - Según la **conceptualización:**
    - ***Perimetral*** *("The walled fortress")*
    - ***Integrada*** *("The open metropolis")*
  - Según la **estrategia:**
    - ***Preventiva*** *(e.g. basada en propiedades)*
    - ***Reactiva*** *(e.g. basada en amenazas)*
  - Según los modelos de adversarios, las capacidades, según los modelos, las tecnologías, las partes, las actividades, etc…

Introducción

- **Seguridad en el ciclo de vida de los S.I.**
  - Definición
  - Viabilidad
  - Requisitos
  - Diseño
    - *Arquitectura*
    - *Adquisición*
  - Realización
    - *Verificación y Validación*
    - *Despliegue*
  - Uso
    - *Adaptación*
    - *Mantenimiento*
  - Evolución

Introducción

- **Soluciones de Seguridad**
  - Las soluciones de seguridad no son obvias, estables, simples, eternas, …
  - Lo que haya funcionado en un contexto o en una situación no tiene porqué funcionar en otros casos.
- **Contexto**
  - Nivel de seguridad
  - Requisitos de seguridad
  - Tecnologías
  - Estabilidad del conocimiento
  - Dinamismo
  - Control

Introducción

- **La ingeniería de seguridad hoy**
  - Las prácticas tradicionales para el desarrollo de sistemas seguros han estado (y siguen estando en muchos casos) **más cerca de ser un arte que una disciplina de ingeniería**.
  - La seguridad se sigue tratando como un añadido y por ello sus actividades de ingeniería **no están integradas en las prácticas de desarrollo de software**.
  - Tener **"artesanos" de seguridad experimentados** sigue siendo esencial para lograr niveles aceptables de seguridad.
  - Varias iniciativas y líneas de investigación han tratado de abordar esta situación con el fin de introducir enfoques que doten de rigor y constituyan una verdadera disciplina de ingeniería para el tratamiento de los aspectos de seguridad en sistemas de información, centrándose principalmente en **ciertas fases** (principalmente las finales) de desarrollo o de algunos **aspectos específicos**.

Introducción

- **Situación actual**
  - **Tenemos soluciones y metodologías de seguridad**, pero…
    - *Frecuentemente nos damos cuenta de que no están adaptadas a lo que necesita "nuestro" sistema*
    - *Las soluciones son complejas / difíciles de entender / las propiedades de seguridad no están bien definidas…*
      - Consecuencia: las decisiones de seguridad se toman ad-hoc (del latín: significa literalmente "para esto" pero en este contexto podéis asumir que significa "como buenamente pueda") → reusabilidad nula, documentación la justa,
  - **Hay formas de especificar los requisitos de seguridad**, pero…
    - *No se hace con la suficiente precisión y detalle*
    - *Asociar requisitos y soluciones es frecuentemente imposible*
  - **Existe la Ingeniería dirigida por modelos**, pero…
    - *El tratamiento de la seguridad es pobre, o está poco integrado, o es simplista, o está limitado … y a veces todo junto*
- **Hay infinidad de escenarios y ejemplos en el mundo real y en la industria que piden a gritos avances en esta línea!**

Ciberseguridad Empresarial

Yo no necesito seguridad…

- Soy pequeño, no tengo nada que sea valioso, no manejo dinero, ….
- Es costoso, no tengo medios, no sé como afrontarlo…
- No merece la pena…
- Los hackers no estarán interesados en mi…
- ¿qué probabilidad hay?

Hechos a considerar

- **La mayoría de los ataques:**
  - no son específicos (targeted attacks)
  - no son "manuales" (robots)
  - no son previsibles
  - cambian continuamente
  - son exhaustivos (hoy se estima que puede recorrer internet entre 4 y 10 horas – hace un año se necesitaban meses)
- **Las empresas grandes detectan más ataques**
- **La ciberguerra no es ciencia-ficción**
- **Los cibermercenarios existen**
- **La pregunta no es ¿me pasará? sino ¿cuándo me pasará?**
  - O incluso ¿me ha pasado ya?

Consecuencias

- **Un solo ataque puede hacer mucho daño o incluso hundir una empresa**
  - Caso Blackberry
  - Caso Ashley-Madison
- **Los ataques pueden costar millones**
  - Caso Sony (2011) → $171 – 270 millones
- **Pérdida de**
  - Tiempo
  - Reputación
  - Oportunidades
  - Dinero
  - …

El lado oscuro existe

A quien nos enfrentamos

- **Motivaciones**
  - Cyber-criminals
  - Hacktivists
  - Governments
  - …
- **¿Qué hacen?**
  - Cyber-espionage
  - Cyber-warfare
  - Cyber-attack outsourced services
  - Exploit kits
  - …

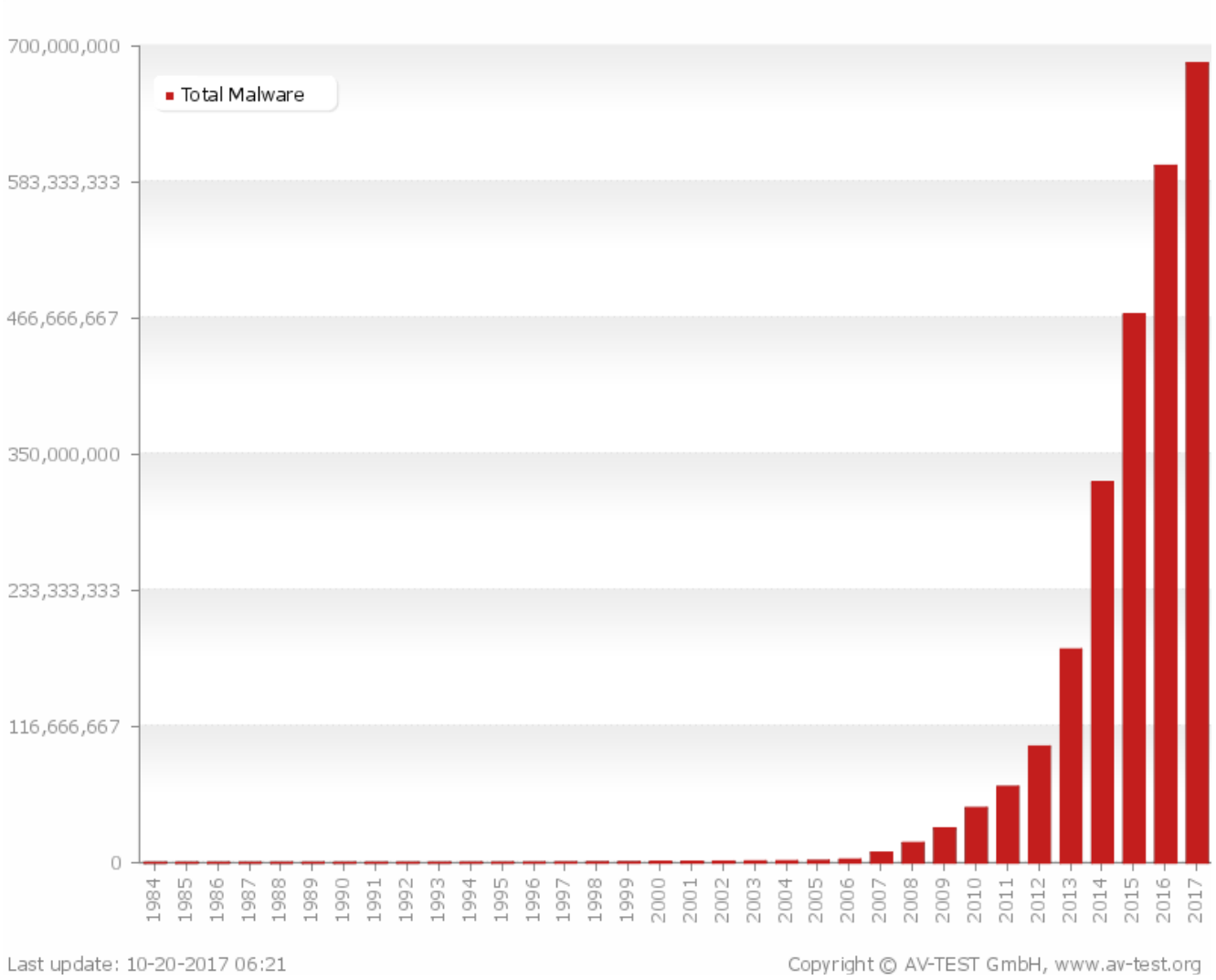
¿Cómo funcionan los ataques?

- **Ataques dirigidos**
  - Se ataca un destino concreto con un fin concreto
  - Se conoce el objetivo (white box)
- **Ataques generales**
  - Se busca un destino cualquiera
  - No se conoce el objetivo (black box)

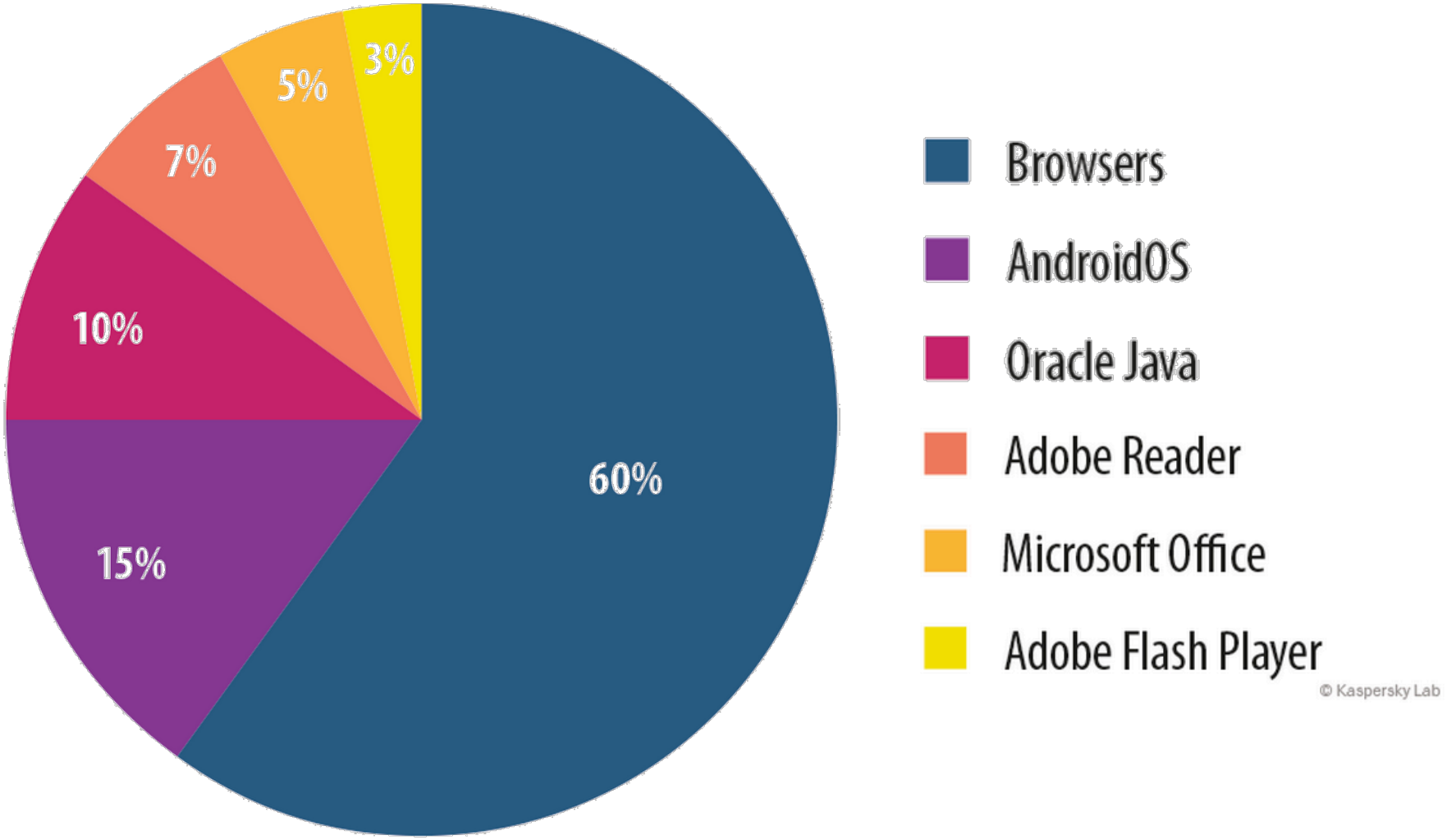
Malware

- **El término Malware, es una abreviatura de MALicious softWARE, y se usa para referirse a cualquier software cuyo objetivo es malicioso:**
  - Destrucción
  - Robo
  - Control
  - Ataques
  - …

¿Cuánto malware?



¿Dónde se esconde el malware?



Caballos de Troya

- **Es más una técnica usada para instalar malware que un tipo de malware como tal.**
- **Se trata de esconder el software malicioso en otro inocuo. Los caballos de Troya necesitan de la acción del usuario para instalarse, pero una vez que lo hacen pasan a desarrollar acciones maliciosas.**

Virus

- **Un programa que normalmente se esconde en otros programas y que es capaz de crear copias de sí mismo. En general, su objetivo es realizar acciones maliciosas o ilegales.**

Spyware

- **Se trata de programas que normalmente se distribuyen como caballos de Troya y que se dedican a enviar información del uso del ordenador a algún servidor remoto.**
- **Normalmente actuan en modo “stealth”. Están inactivos (en cuanto a conexiones) hasta que sucede algo y en ese momento envían la información al servidor**

Adware

- **Se trata de programas que normalmente se distribuyen como caballos de Troya y que se dedican a generar beneficios para el autor, por ejemplo, mediante la intercepción de los clicks que el usuario realiza en su navegación normal.**
- **En este caso, los distribuidores intentan disfrazar el software en forma de alguna utilidad (p. ej. barras de navegadores) y describen su funcionalidad en términos poco detallados. En realidad se trata de un software "legal" (esto es, es difícil interponer denuncias legales contra este tipo de software). Su desinstalación suele ser compleja.**

Ransomware

- **Se trata de malware que cifra la información de la víctima y luego pide un "rescate" económico por su recuperación.**
- **Se ha popularizado últimamente**
- **Hay varios casos llamativos conocidos**
- **Se deduce que hay muchos casos que no se han hecho públicos**

Rootkits

- **Malware que se oculta en el SO del equipo infectado. Este tipo de malware es muy dificil de detectar, excepto por sus efectos, y también suele ser difícil de eliminar.**
- **Suele tener mecanismos para evitar su eliminación, que a veces sólo es posible haciendo que el sistema se bloquee (crash).**

Backdoors

- **Malware que instala un medio de acceso al equipo infectado saltándose los mecanismos normales de seguridad y control de acceso.**
- **El software suele instalar más de una puerta trasera, y puede quedar en espera durante bastante tiempo sin que el sistema tenga síntomas de ello.**
- **Hay numerosas historias sobre puertas traseras instaladas por fabricantes y gobiernos.**

Y hay más…

- **Phishing,**
- **Cyber bullying,**
- **Cyber espionage,**
- **Deep web,**

- **Anonimizadores (Onion routing),**
- **etc.**

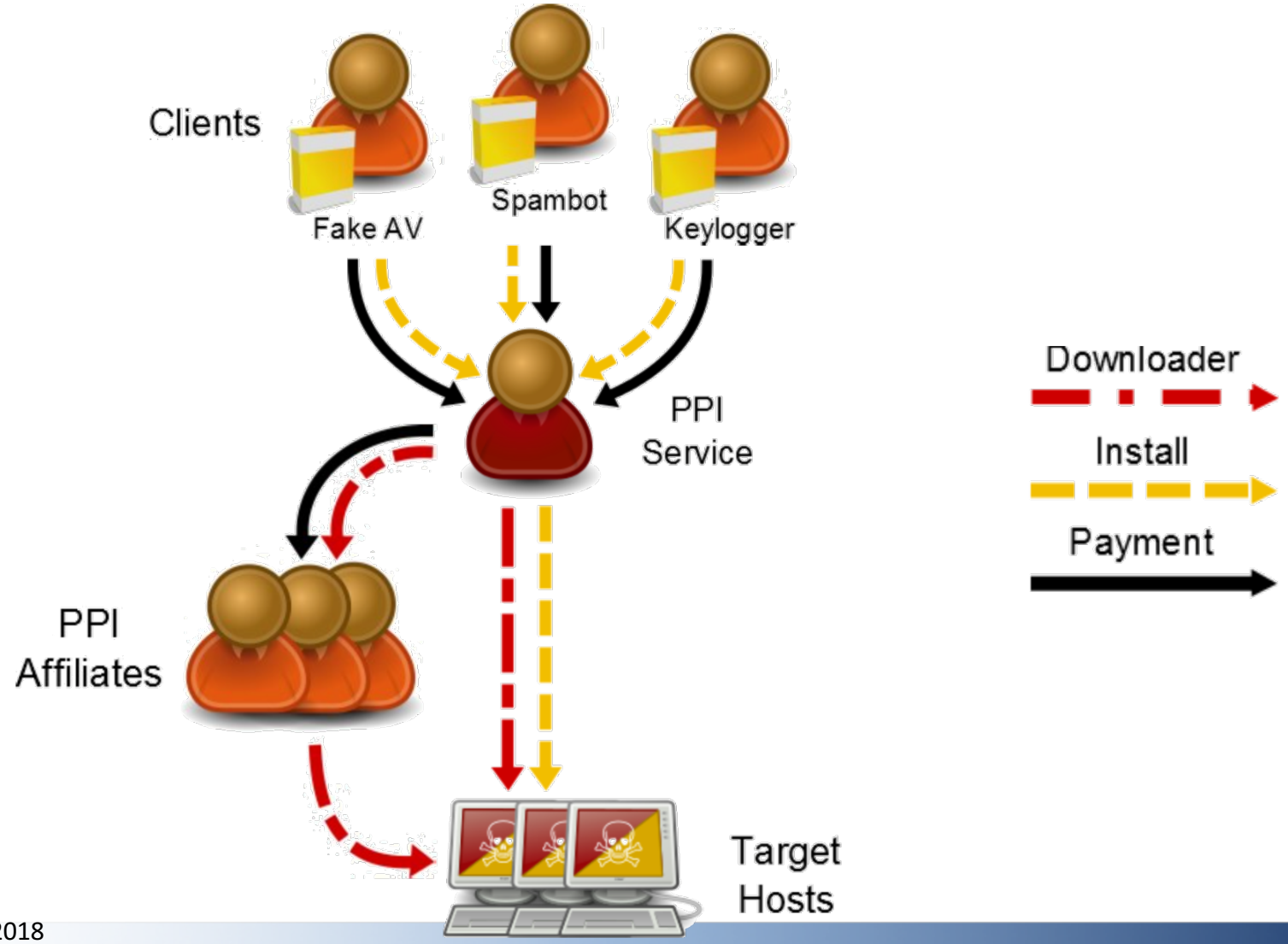
Técnicas de ocultación

- **Técnicas usadas para evitar la detección y eliminación**
  - Target Fingerprinting
  - Randomized homomorphic code modification
  - Timing-based evasion
  - Obfuscation

Outsourced attacks

- **Como todo outsourcing, se trata de delegar el ataque a una entidad externa experta en estas tareas**
- **Puede ser directo o mediante otros medios como PPI (Pay per install), Exploit kits, Drive-by download.**

PPI Malware


Clients
Fake AV
Spambot
Keylogger
PPI
Service
PPI
Affiliates
Target
Hosts
Downloader
Install
Payment

¿Cuánto cuesta el outsourcing?

Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$
IT	65$
CH	20$
CZ	20$

Exploit kits

- **Paquetes de software listos para usarse en ataques**
- **Los hay que se instalan con software “normal”**
  - Java
  - Browsers
  - Flash
- **Otros se instalan en servidores**

Correo basura (Spam/Junk mail)

- **Spam = email masivo no solicitado**
  - Anuncios
  - Virus
  - Phishing
  - Spyware
  - Timos varios…
- **Problemas**
  - Volumen / Molestia
  - Costes
  - Pérdida de recursos
  - Fraude

Ataques de Ingeniería social

- **Se trata de una de las técnicas más efectivas para desplegar ataques porque se centra en uno de los puntos más débiles en la cadena: los humanos.**
- **La idea es hacer que el propio usuario sea el que realice la acción que inicia o constituye el ataque.**

Ataques desde dentro

- **En los últimos años constituyen el mayor número de ataques dirigidos**
- **Iniciados o realizados en colaboración con empleados o ex-empleados**
- **Pueden prepararse con mucho tiempo**
- **Pueden lanzarse mucho después de que el empleado haya dejado la empresa**
- **Son los que más daño hacen**
  - Caso Ashley Madison

¿De dónde surgen los problemas?

Amenazas

- **Amenaza # 10: Ataques desde adentro**
  - Control dual
  - Separación de funciones
- **Amenaza # 9: Falta de contingencia**
  - Inversión
- **Amenaza # 8: Mala configuración**
  - Auditoría
- **Amenaza # 7: Uso temerario de redes de hoteles y quioscos**
  - Política de uso de servicios de IT
  - Firewalls
- **Amenaza # 6: Uso imprudente de hotspots inalámbricos**
  - Política de uso de servicios de IT
  - Firewalls

Fuente: www.watchguard.com

Amenazas

- **Amenaza # 5: Datos perdidos en un dispositivo portátil**
  - Selección y Administración de dispositivos en base a la seguridad
- **Amenaza # 4: Servidores Web comprometidos**
  - Servicios de "desestandarización"
  - Auditoría, monitorización
- **Amenaza # 3: Navegación imprudente por parte de los empleados**
  - Filtros de contenidos web.
- **Amenaza # 2: Correo electrónico HTML malicioso**
  - Filtros anti-spam
  - Filtros de correo
- **Amenaza # 1: Explotación automática de una vulnerabilidad conocida**
  - Actualización responsable y continua

Fuente: www.watchguard.com

Amenazas

- **Amenaza # 0: Las personas**
  - Dentro y fuera de la organización
  - Consciente e inconscientemente
  - Relación con la situación laboral
  - …

¿Qué herramientas tenemos?

Estrategias

- **Pólizas de Ciber-seguridad**
  - Caras, cobertura insuficiente, poco claras…
- **In-house cyber-security operations center (SOC)**
  - Chief Information Security Officer (CISO)
  - Parte del departamento de informática vs. Departamento específico
- **Outsourced security management**
  - Managed SecurityProviders (MSPs)

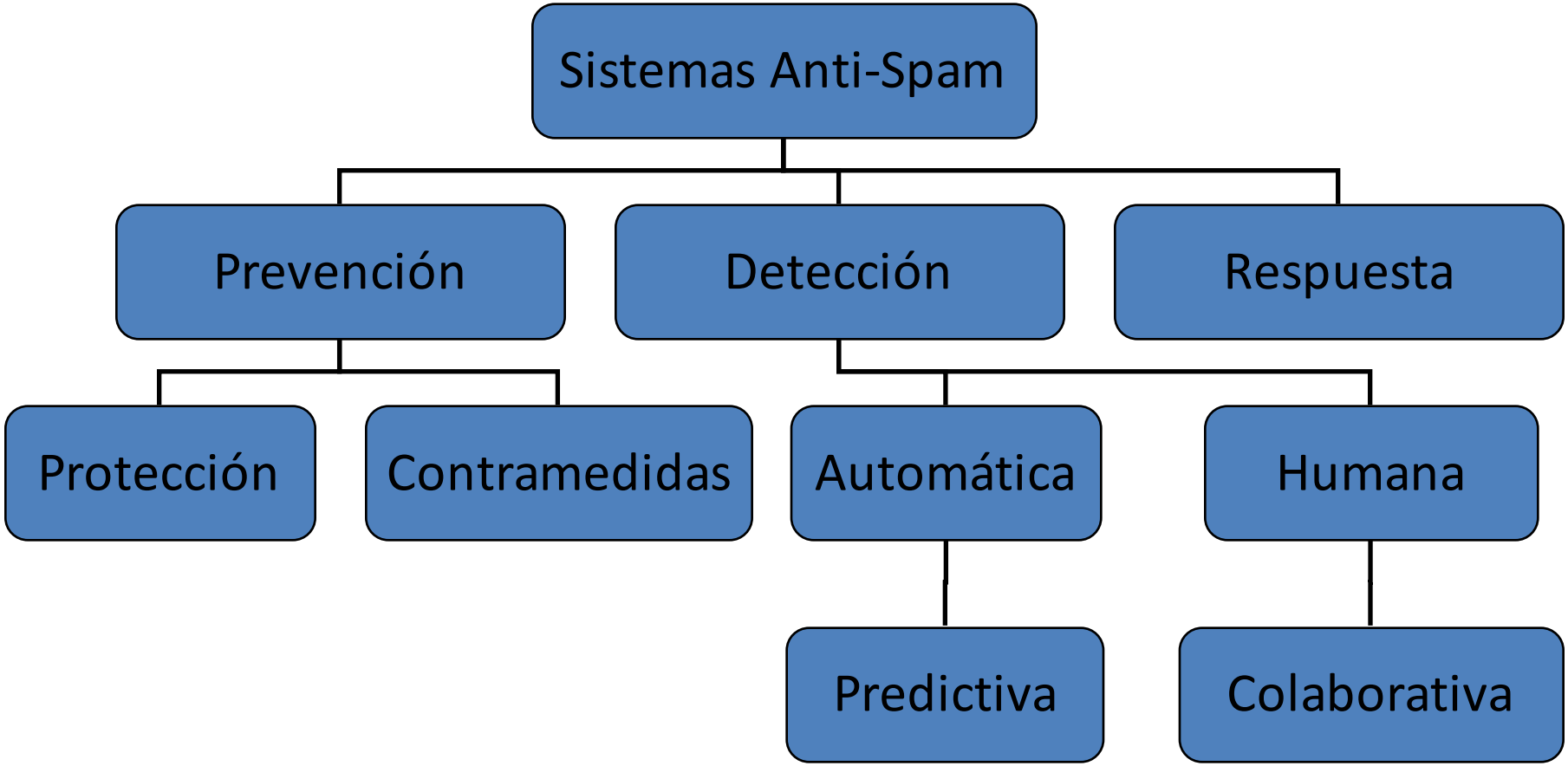
Medidas de alto nivel

- **Formación**
- **Documentación**
- **Identificación de recursos**
- **Análisis de riesgos**
- **Análisis de ciberseguridad**
- **Plan de ciberseguridad**
- **Plan de contingencia**

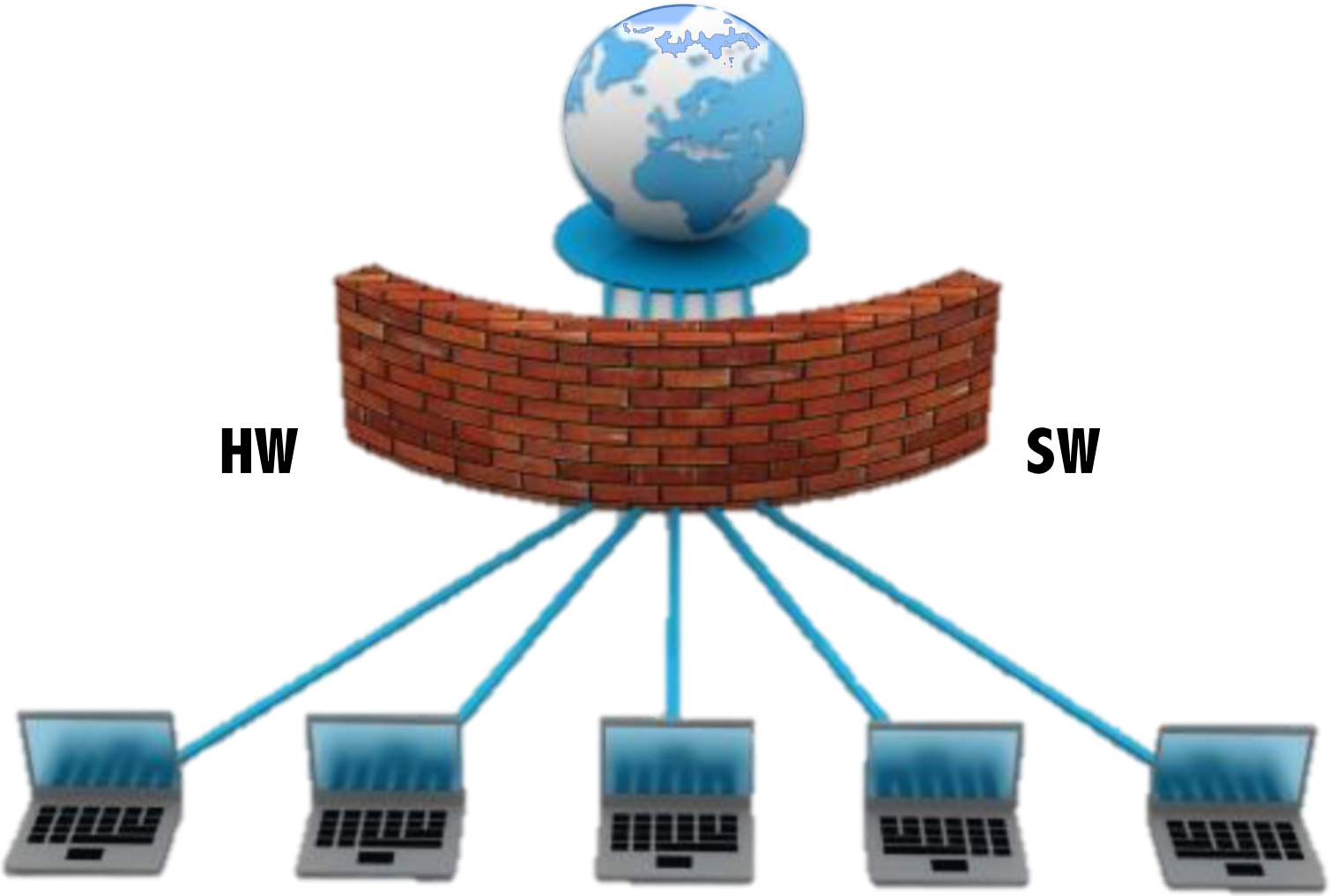
Políticas

- **P4sswords**
  - Caso Hacking Team
- **Configuración Software**
- **BYOD**
- **Sitios Web**
- **Servicios Web**
- **Mantenimiento de equipos**
- **Gestión de personal**
- **Formación**

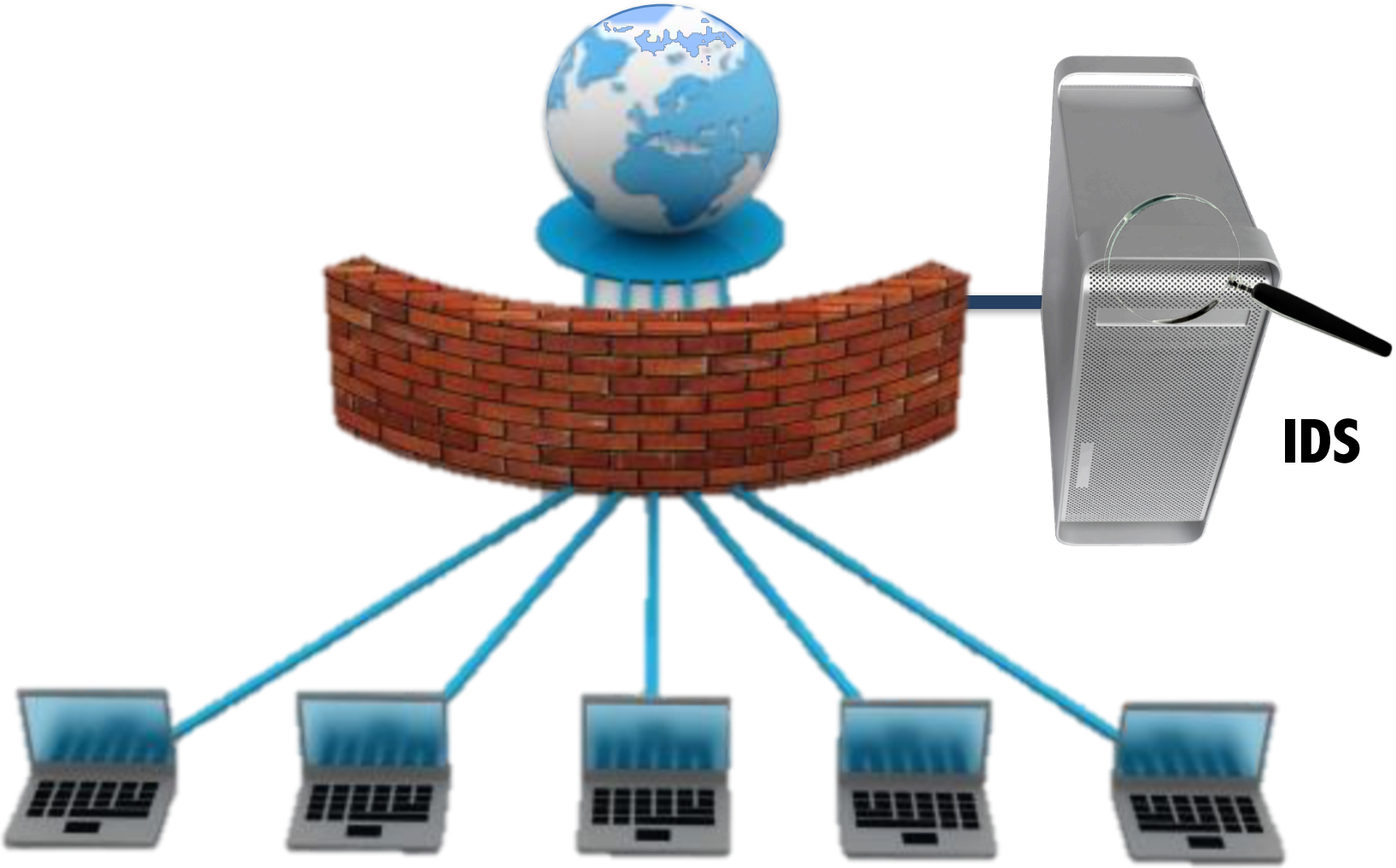
Sistemas Anti-Spam



Cortafuegos (Firewalls)



Sistemas de Detección de Intrusos (IDS)



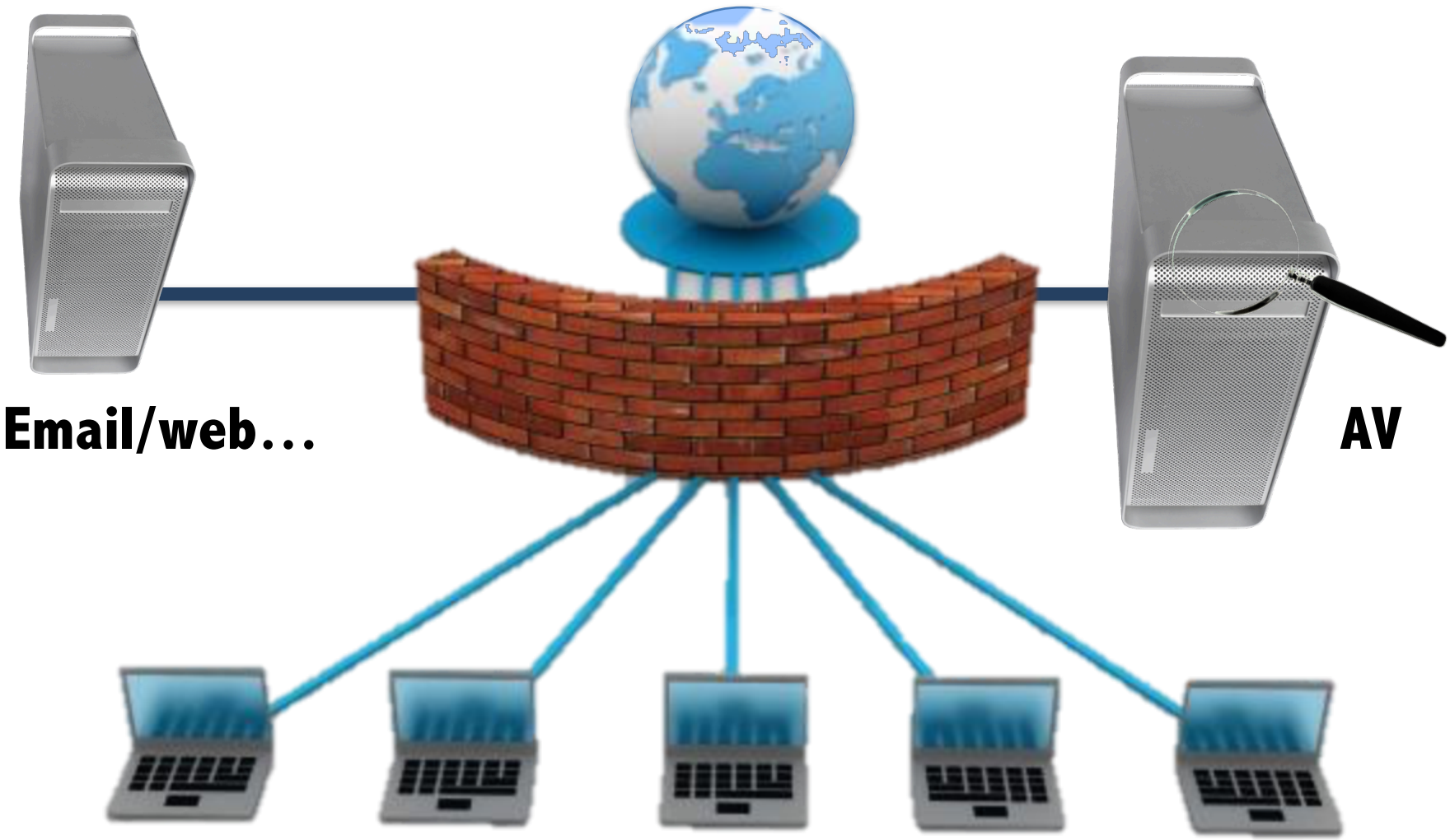
Antivirus

- **Locales**
- **Corporativos**

- **Tener antivirus es una necesidad reconocida**
  - Se cumple generalmente
  - Un antivirus mal mantenido no sirve
    - *No merece la pena*

- **No hay antivirus que pueda evitar tantos problemas como un uso cuidadoso de los equipos**

Antivirus corporativo



Autenticación vs. Autorización

- **Autenticación: se demuestra quién se es**
  - Alternativas:
    - *algo que SE ES,*
    - *algo que SE TIENE,*
    - *algo que SE SABE*
- **Autorización: se demuestra qué se es o qué se puede hacer**
  - La Autorización se basa a veces en la Autenticación,
  - Por lo tanto, trata sobre los derechos o privilegios que se poseen para realizar una tarea o acceder a un recurso
- **El control de acceso limita qué usuarios acceden a qué recursos y para qué**

Modelos de control de acceso

MAC, *Mandatory Access Control*

- Entornos militares
  - *Gran número de usuarios*
  - *Jerarquía lineal predeterminada y estática*
- Control basado en Nivel de Seguridad
  - *Reglas definidas por una autoridad central*
  - *Niveles predefinidos*
  - *Los usuarios y los recursos se asocian a un nivel*
  - *Hay variantes con transitividad y sin ella*
  - *Hay variantes con reglas de lectura/escritura diferentes*

Modelos de control de acceso

DAC, *Discretionary Access Control*

- BD Multiusuario
  - *Número reducido de usuarios conocidos*
  - *Cambios poco frecuentes*
  - *Recursos centralizados*
- Control basado en la identidad
  - *Reglas que determinan lo que cada usuario puede hacer*
- Ejemplo: Permisos UNIX

Modelos de control de acceso

RBAC, *Role-based Access Control*

- Desarrollado para redes corporativas
  - *Se definen estructuras jerárquicas de categorías de usuarios (roles)*
  - *Puede haber herencia*
  - *Las reglas de acceso asocian permisos a los roles*
  - *Los usuarios se asocian a los roles que pueden tomar (normalmente por identidad)*
- Control basado en el rol del usuario
  - *Hace falta un rol por cada clase de equivalencia de recursos en cuanto a permisos*
  - *La gestión de roles es compleja y dada a errores*
  - *La gestión de roles es poco dinámica*

Modelos de control de acceso

SAC, Semantic *Access Control*

- Desarrollado para redes corporativas
  - *Se basa en el concepto de atributo*
  - *Se asignan atributos a los usuarios (normalmente mediante certificados)*
  - *Las reglas de acceso asocian permisos a conjuntos de atributos*
  - *Se permiten accesos anónimos*
- Control basado en los atributos del usuario
  - *Hay tantas clases de equivalencia como combinaciones de atributos*
  - *La gestión es sencilla y verificable automáticamente*
  - *La gestión es dinámica*

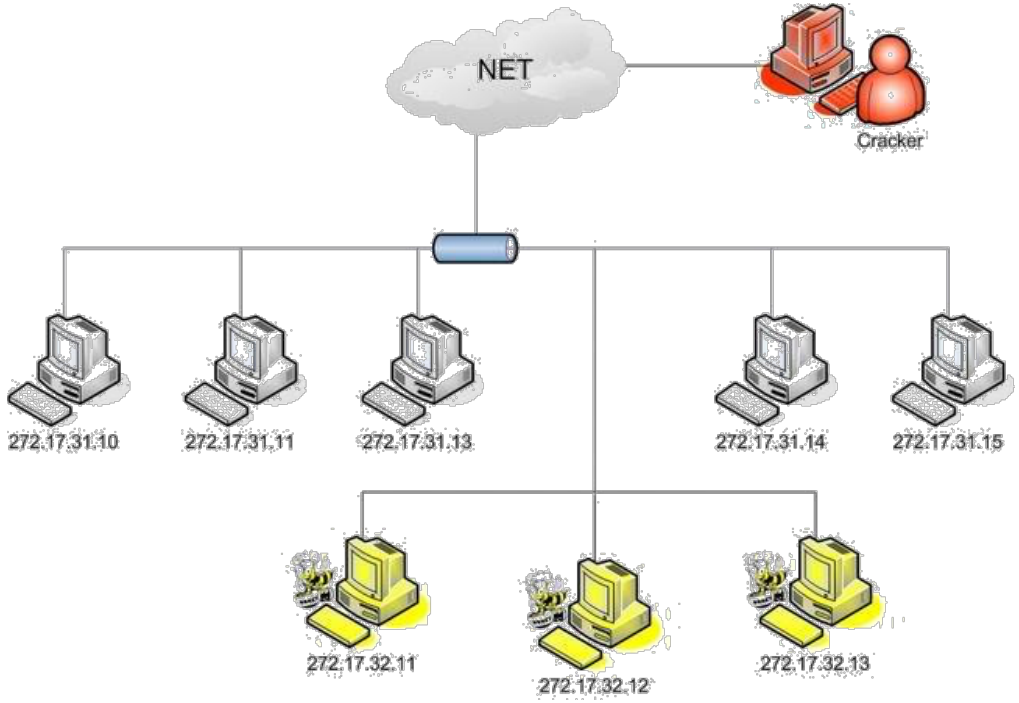
Trampas (Honeypots)

- **En el mundo del espionaje el término se refiere al uso de seducción sexual para reclutar agentes, o para engañar a agentes enemigos**

Trampas (Honeypots)

- **Se trata de preparar una serie de equipos que "llaman" a los atacantes mediante "señales" de debilidad**

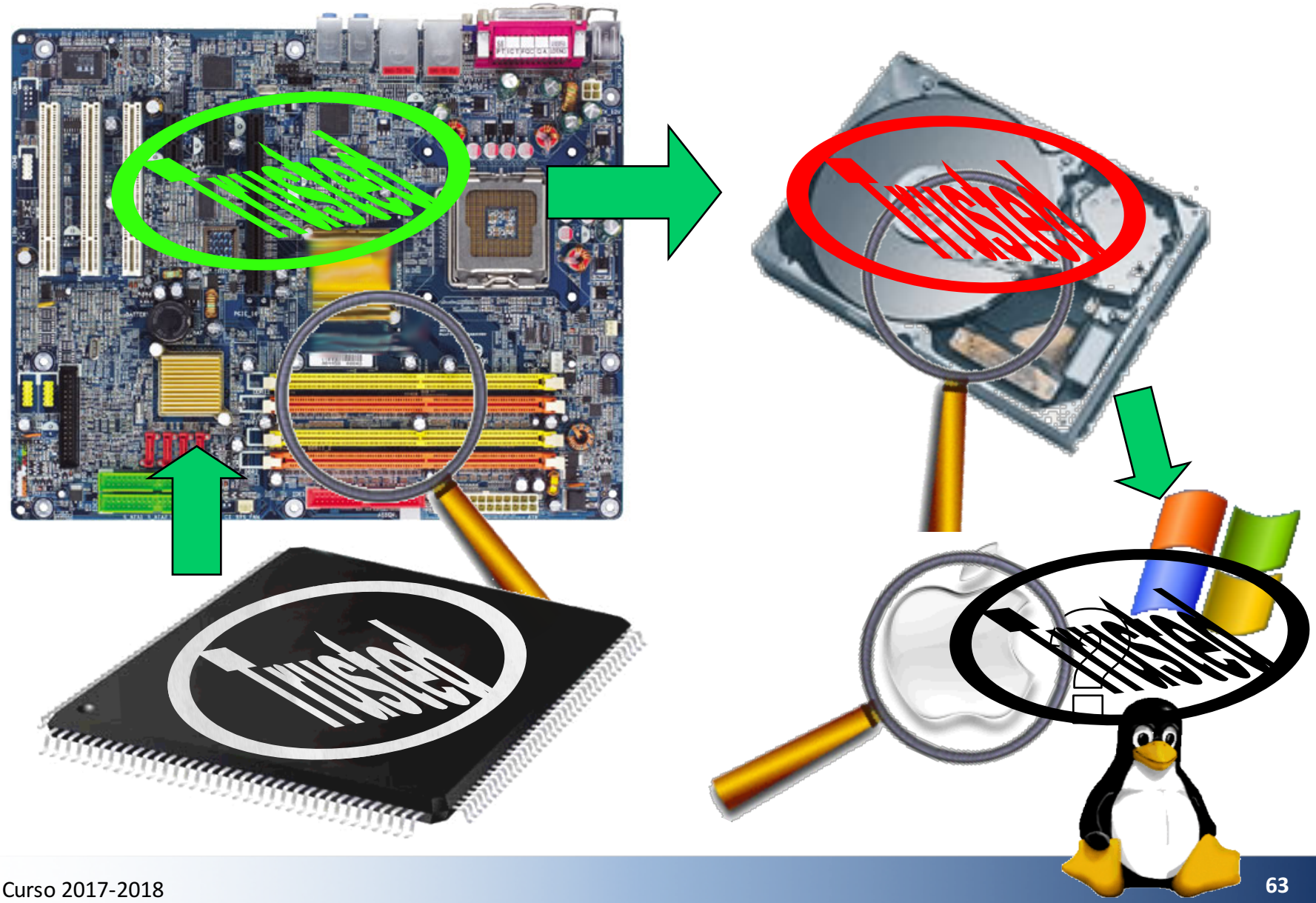
- **Estos equipos están monitorizados**
- **Objetivos**
  - Distraer a los atacantes de los recursos valiosos
  - Aprender / Detectar zero-day exploits
  - Ganar tiempo de reacción
  - Detectar ataques desde dentro



Copias de seguridad (Backups)

- **Las copias de seguridad pueden ser un elemento importante en la seguridad.**
- **Pueden ser esenciales en la capacidad de restaurar el servicio**
- **Pueden ser cruciales en los análisis forenses post-mortem de un sistema atacado**
- **Pueden evitar males mayores en algunos casos como por ejemplo ante ransomware**

Trusted Computing

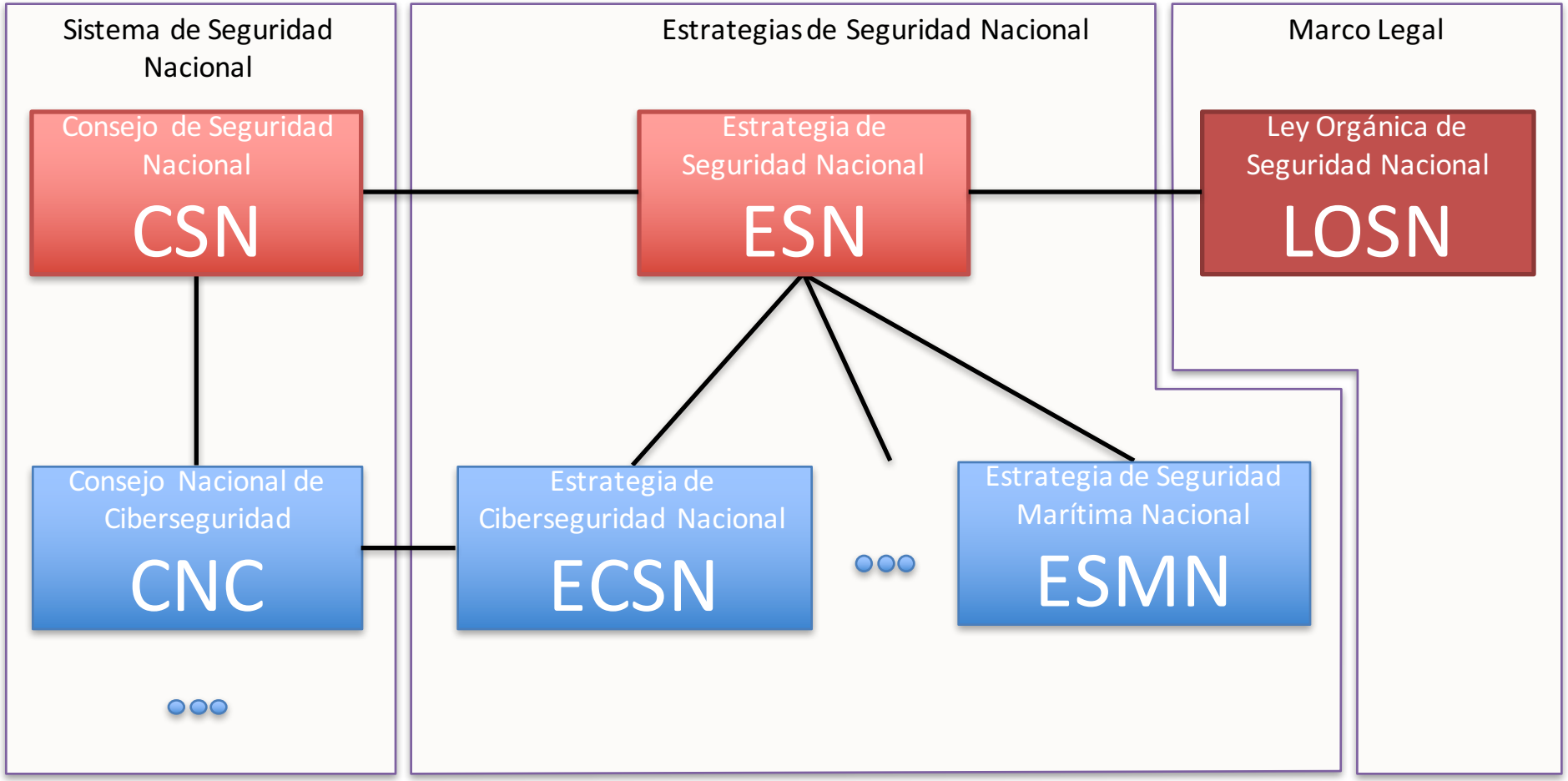


Security / Privacy-by-design

- El desarrollo de aplicaciones y servicios corporativos no puede afrontarse como un "upgrade" de desarrollos "de juguete" o "de prueba"
- Las prisas pueden jugar malas pasadas
- En general posponer el diseño de la seguridad es garantía de problemas
- Hay que ser consciente de los riesgos en los que se incurre cuando se añade una nueva aplicación o servicio

Estrategia de Ciberseguridad Nacional

Marco


Sistema de Seguridad Nacional
Consejo de Seguridad Nacional
CSN
Consejo Nacional de Ciberseguridad
CNC
Estrategias de Seguridad Nacional
Estrategia de Seguridad Nacional
ESN
Estrategia de Ciberseguridad Nacional
ECSN
Estrategia de Seguridad Marítima Nacional
ESMN
Marco Legal
Ley Orgánica de Seguridad Nacional
LOSN

¿Qué es y para qué sirve la ECSN?

- En los últimos años los principales países desarrollados, especialmente en Europa, Norteamérica y en la órbita de la Unión Europea y de la OTAN, han venido publicando sus Estrategias Nacionales de Ciberseguridad.
- Una Estrategia Nacional de CiberSeguridad es un documento que recoge la visión del gobierno de una nación a la hora de enfrentar el problema de la gestión de la Ciberseguridad en el ámbito global de dicha nación.
- Todas responden a un mismo esquema que consiste en la definición de unos objetivos nacionales respecto a la gestión de la Ciberseguridad y unas líneas de actuación para alcanzar esos objetivos en un determinado plazo.

¿Qué es y para qué sirve la ECSN?

- **Estructura y planteamiento:**
  - Motivación, estado actual de la Ciberseguridad
  - Objetivos a conseguir
  - Líneas de actuación
  - Organización
  - Presupuesto
- **España ha sido uno de los últimos países en publicar su Estrategia Nacional de Ciberseguridad, a finales del 2013:**
  - El ciberespacio y su seguridad
  - Propósito y principios rectores de la Ciberseguridad en España
  - Objetivos de la Ciberseguridad
  - Líneas de Acción de la Ciberseguridad
  - La Ciberseguridad en el Sistema de Seguridad Nacional
- **No incluye la dotación presupuestaria.**

¿Qué es y para qué sirve la ECSN?

- **La Estrategia de Ciberseguridad Nacional busca mejorar e impulsar la ciberseguridad en España.**
  - Perspectiva integral.
  - Todos los agentes (públicos y privados).
  - Protección de los activos nacionales, incluidas empresas estratégicas.
  - Se divide en diversas iniciativas, para las que se crea un plan identificando los organismos responsables de su diseño y ejecución, la legislación de referencia así como las medidas de carácter técnico que están siendo aplicadas.

¿Quiénes son los responsables?

- **Ministerio del Interior.**
  - Infraestructuras Críticas.
  - Ciberdelito.
  - Ciberterrorismo.
- **Ministerio de Defensa.**
  - Sus propios sistemas información y telecomunicaciones.
  - Sistemas de interés Defensa Nacional que se le asignen.
  - Acciones ofensivas.
- **Centro Criptológico Nacional.**
  - Administraciones Públicas.
- **Ministerio de Industria.**
  - Empresas públicas y privadas.

Privacidad en NE

Privacidad

- **Seguridad ≠ Privacidad**

- **Autenticidad**
- **Integridad**
- **Confidencialidad**
- **No repudio**

} **Seguridad**

- **Privacidad**
  - Protección de datos

(Tratamiento justo de la información)

Niveles de Idenfificación

Privacy stages	identifiability	Approach to privacy protection	Linkability of data to personal identifiers	System Characteristics
0	identified	privacy by policy (notice and choice)	linked	• unique identifiers across databases • contact information stored with profile information
1	pseudonymous		linkable with reasonable & automatable effort	• no unique identifies across databases • common attributes across databases • contact information stored separately from profile or transaction information
2		privacy by architecture	not linkable with reasonable effort	• no unique identifiers across databases • no common attributes across databases • random identifiers • contact information stored separately from profile or transaction information • collection of long term person characteristics on a low level of granularity • technically enforced deletion of profile details at regular intervals
3	anonymous	privacy by design	unlinkable	• no collection of contact information • no collection of long term person characteristics • *k*-anonymity with large value of *k*

Sarah Spiekermann and Lorrie Faith Cranor. **Engineering Privacy.** IEEE Transactions on Software Engineering. Vo. 35, No. 1, January/February, 2009, pp. 67-82. http://ssrn.com/abstract=1085333

Ejemplos de herramientas para privacidad

- **Cookie managers**
- **Anti-Rastreadores**
- **Anonymizers**
  - Web browsers
  - Onion routing
- **Privacy publishing**
  - Project Maelstrom
- **Cifrado**
- **Utilidades de "limpieza" de discos**
- **P3P (http://www.w3.org/P3P)**
  - Platform for Privacy Preferences (P3P) Project

Laptop Compubody Sock for privacy, warmth, and concentration in public spaces

Created by Becky Stern http://sternlab.org/2008/04/body-technology-interfaces/

Consideraciones

- **La privacidad es un aspecto secundario**
  - Los usuarios pueden querer usar herramientas de privacidad, pero siempre centrarán su atención en la actividad principal
    - *Comprar, Buscar, Comparar, Comunicar…*
- **Muchas soluciones de privacidad reducen la funcionalidad, comodidad o rendimiento de las aplicaciones**
- **La privacidad tiene un componente personal alto**
  - Cada usuario tiene sus preferencias y criterios
  - No valen las soluciones "talla única"
- **La mayoría de usuarios no son expertos en privacidad**
  - Es dificil que entiendan las implicaciones presentes y futuras de sus acciones
  - Es dificil explicarles las opciones de privacidad existentes
  - Es dificil entender sus criterios y preferencias

El “consentimiento informado”

- **Los usuarios deben consentir EXPLÍCITAMENTE en la cesión de datos**
  - Qué
  - Para qué
  - Quien
  - Cuando (hasta cuando)
  - Cómo

- **Consentimiento INFORMADO requiere que los puntos anteriores se definan de forma clara e inteligible**

Política de Proteccion de Datos y Privacidad

(Consentimiento informado)

En esta Sección se expone la Política de Privacidad que regula el uso del servicio del sitio web que XXXXX pone a la disposición de los usuarios de Internet, sobre la información de carácter personal que puede facilitar cuando visita nuestra página web.

1. Uso y Tratamiento de datos de carácter personal

- **En cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), XXXXX le informa que los datos de carácter personal proporcionados mediante la cumplimentación de los correspondientes formularios de registro electrónico contenidos en el portal, de las consultas referentes a los servicios ofrecidos, así como aquellos datos a los que XXXXX acceda como consecuencia de su navegación, serán incorporados en los archivos automatizados de la entidad, pudiendo ejercitar su derecho de acceso, rectificación, cancelación y oposición al tratamiento de sus datos en los términos y condiciones previstos en el apartado 3º.**
- **Por otra parte, mediante el registro de los datos, el usuario otorga su consentimiento al tratamiento de los mismos con las finalidades señaladas.**
- **En aquellos casos donde sea necesario cubrir un formulario y realizar el envío, su realización implicará necesariamente que fue informado (en virtud del artículo 5 LOPD) y, en su caso, otorgó el correspondiente consentimiento (la tenor del artículo 6 LOPD) al contenido de la cláusula anexada al formulario y a la presente política de privacidad.**
- **El usuario deberá rellenar los formularios con datos verdaderos, exactos, completos y actualizados, siendo informado en ese preciso momento de aquellos datos de obligada cumplimentación (*) y sus consecuencias en caso de no hacerlo. Asimismo, con la aceptación, reconoce que la información y los datos personales recabados son exactos y veraces.**
- **Rogamos comunique de forma inmediata a XXXXX cualquier modificación de sus datos de carácter personal, a fin de que la información contenida en los archivos municipales, esté en todo momento actualizada y no contenga errores o desactualizaciones.**

Política de Proteccion de Datos y Privacidad

2. Medidas de Seguridad

- **XXXXX le informa que tiene implantadas las medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de sus datos de carácter personal y evitar su alteración, pérdida y tratamiento y/o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o de en medio físico o natural. Todo eso, de conformidad con lo previsto en el artículo 9 de la LOPD y en el Real Decreto 994/1999, de 11 de junio, por lo que se aprueba la Legislación de Medidas de Seguridad de los Archivos Automatizados que contengan Datos de Carácter Personal (RMS).**
- **Así, XXXXX ha establecido medidas adicionales en orden a reforzar la confidencialidad e integridad de la información en las organizaciones, como el establecimiento de limitaciones al uso del correo electrónico a la hora de enviar datos o documentos de carácter confidencial. No obstante, el usuario debe ser consciente de que las medidas de seguridad en Internet no son inexpugnables.**
- **XXXXX continuamente mantiene la supervisión, control y evaluación de los procesos para asegurar el respeto a la privacidad de los datos.**

3. Ejercicio de derechos: Acceso, Rectificación, Cancelación y Oposición.

- **Aquellas personas físicas que faciliten sus datos a XXXXX podrán dirigirse a esta administración, en su calidad de Responsable del archivo, con el fin de poder ejercitar gratuitamente sus derechos de acceso, rectificación, cancelación y oposición respeto de los datos incorporados en sus archivos en los términos previstos por la legislación vigente .**
- **Dado el carácter confidencial de la información, usted no podrá ejercitar sus derechos telefónicamente, debido a que este medio no permite acreditar la identidad como titular de los datos registrados.**
- **El interesado podrá ejercitar sus derechos mediante comunicación por escrito dirigida al XXXXX , con la siguiente referencia en su carta: "LOPD Ejercicio de derechos" (junto a su solicitud escrita y firmada, deberá acreditar su personalidad aportando fotocopia del D.N.I)**

Política de Proteccion de Datos y Privacidad

4. Uso de Cookies

- Las "cookies" constituyen una herramienta empleada por los servidores Web para almacenar y recuperar información aportada por sus usuarios. No es más que un archivo de texto que algunos servidores piden al navegador que escriba en su disco duro, con información aportación de las acciones realizadas por la página.
- Poseen una fecha de caducidad, que puede oscilar desde el tiempo que dure la sesión incluso una fecha futura especificada, a partir de la cual dejan de ser operativas.
- Para mayor información, visite el site del Departamento de Tratamiento de la Información y Codificación dependiente del Consejo Superior de Investigaciones Científicas de España.
- XXXXX utiliza "cookies" para la personalización de los servicios ofrecidos a los usuarios.
- Las "cookies" empleadas por XXXXX se utilizan para permitir la identificación de usuarios registrados y no pueden leer datos de su disco duro ni incluir virus en sus textos.
- Asimismo, XXXXX no puede leer las "cookies" implantadas en el disco duro del usuario desde otros servidores.
- En este sentido, el usuario pode configurar su navegador para aceptar o rechazar por defecto todas las "cookies" o para recibir un aviso en pantalla de la recepción de cada "cookie" y decidir en ese momento su implantación o no en su disco duro. Para eso le sugerimos consultar la sección de ayuda de su navegador para saber como cambiar la configuración que actualmente emplea.
- Aun cuándo el usuario configurara su navegador para rechazar todas las "cookies" o rechazara expresamente las "cookies" de XXXXX podrá navegar por el Portal con el único inconveniente de no poder disfrutar de las funcionalidades del Portal que requieran la instalación de alguna de ellas.
- En cualquiera caso, el usuario podrá eliminar las "cookies" implantadas en su disco duro en cualquier momento, siguiendo el procedimiento establecido en la sección de ayuda de su navegador.
- Esta página web utiliza Google Analytics, un servicio de análisis de estadísticas web proporcionado por Google, Inc., una compañía de Delaware con sed principal en 1600 Amphitheatre Parkway, Mountain View (California), QUE 94043, Estados Unidos ("Google"). Google Analytics utiliza cookies, que son archivos de texto situados en el ordenador del usuario para ayudar al sitio web a analizar el uso que hacen los visitantes de nuestra página. La información que genera la cookie acerca del uso del website (incluyendo su dirección IP) será directamente transmitida y archivada por Google en los servidores de Estados Unidos. Google usará esta información y nos la presentará con el propósito de hacer un seguimiento del uso que se hace de nuestra página web recopilando informes de la actividad del site.
- Google podrá transmitir dicha información a terceros cuándo así se lo requiera la legislación, o cuándo terceros procesen la información por cuenta de Google. La política de privacidad de Google puede ser consultada en http://www.google.com/intl/eres/privacypolicy.html.

Política de Proteccion de Datos y Privacidad

5. Enlaces

- **La página corporativa ofrece enlaces la otros Web sites que pueden resultar de su interés. Aunque XXXXX trata de asegurar que los web sites de terceros cumplan los estándares adecuados en seguridad, no podemos garantizar el cumplimiento de la normativa vigente en protección de datos en los mismos.**
- **XXXXX no asume ningún tipo de responsabilidad, ni siquiera de forma indirecta o subsidiaria, por los daños y perjuicios de toda clase que pudieran derivarse del acceso, mantenimiento, uso, calidad, licitud, fiabilidad y utilidad de los contenidos, informaciones, comunicaciones, opiniones, manifestaciones, productos y servicios existentes y ofrecidos en los sitios Web no gestionados por esta administración y que resulten accesibles a través del Portal del XXXXX . No obstante, esta administración se encuadra dentro del apartado a) del artículo 17 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE), ya que esta administración respecto a enlaces facilitados en el Web, no tienen conocimiento efectivo de que la actividad o la información a la que remite o recomienda es ilícita o lesiona bienes o derechos de un tercero susceptibles de indemnización.**

6. Modificación de la política de privacidad.

- **XXXXX se reserva el derecho a modificar su Política de Privacidad de acuerdo a su propio criterio, o motivado por un cambio doctrinal de la Agencia Española de Protección de Datos, legislativo o jurisprudencial. Cualquier modificación de la Política de Privacidad será publicada por lo menos diez días antes de su efectiva aplicación. El uso del Web después de dichos cambios, implicará la aceptación de estos.**

Ejercicio práctico

- **Se trata de preparar un documento de análisis de seguridad y privacidad con:**
  - Análisis de requisitos de seguridad y privacidad
    - *Identificación y descripción de los requisitos de seguridad y privacidad de vuestro negocio electrónico*
    - *Para cada requisito:*
      - Las soluciones elegidas
      - La estimación del impacto en vuestro sistema
  - Plan de cumplimiento de obligaciones legales
  - Documentos base
    - *Terms and Conditions, Disclaimers, legal notice, user license/contract*